THE OFFICE OF THE STATE CHIEF INFORMATION OFFICER
ENTERPRISE TECHNOLOGY STRATEGIES

North Carolina Statewide Technical Architecture

Network Domain

NORTH CAROLINA STATEWIDE TECHNICAL ARCHITECTURE

Network Domain

Date Approved by IRMC:	July 1, 1997	Version:	1.5.7
Revised Date:		Version:	
Revision Approved Date:			
Date of Last Review:	March 17, 2004		
Date Retired:			
Reviewer Notes – Reviewed and updated office title and copyright date. Added a hyperlink for the ETS email – March 17, 2004.			

Office of the State Chief Information Officer
Enterprise Technology Strategies
PO Box 17209
Raleigh, North Carolina 27619-7209
Telephone: (919) 981-5510
E-mail: ets@ncmail.net

Network Domain Principles

Principle 3.00.01.01 – The network provides a communications infrastructure for distributed computing.

Rationale:

- The world is increasingly connected. A network environment provides access to a wide spectrum of information, applications, and resources.
- Any product or application not architected for a networked environment is limited long-term.
- The network provides the delivery mechanism for distributed services in an n-tier architecture.

Principle 3.00.01.02 – A single integrated wide area network (WAN) is the backbone of an enterprise architecture and supports a variety of communication requirements including voice, data, image, and video.

Rationale:

- It allows access to a wide spectrum of information, application and system resources regardless of location or business unit. Thus, access to resources can be obtained in a timely and efficient manner by appropriate requesters when and where needed throughout the enterprise.
- It expands the scope of an organization domain by allowing them to reach out to customers and suppliers through access to the Internet and through the provision of dial-in/dial-out services.
- It acts as the delivery mechanism for the distributed computing services required by the fast-paced, dynamic business.

Principle 3.00.01.03 – Networks should be available seven days a week and twenty-four hours a day.

Rationale:

- Networks provide an increasingly important and necessary role in the execution of business functions and processes. The availability of the network seven days a week and twenty-four hours a day must be maintained in a consistent and complete manner.
- Networks consist of and rely on many interrelated and often highly complex components distributed across a wide geographic area. Failure of any single component can have severe adverse effects on one or more business applications or services.
- Reliable networks contain no single point of failure. Networks are comprised of many components, and are only as reliable as the weakest link. Reliability must be built-in, not added-on.
- Bandwidth must be sufficient to accommodate new and expanding applications, different types of data (e.g., voice, data, image, and video), and a variety of concurrent users.
- The network must support software distribution and installation to a widely dispersed user community.

- The network must be designed to minimize latency. Data must pass across the network in a timely manner so that business decisions can be based on up-to-date information.

Principle 3.00.01.04 – A statewide network must be based on common, open, vendor-neutral protocols.

Rationale:

- An open, vendor-neutral protocol provides the flexibility and consistency that allows agencies to respond more quickly to changing business requirements.
- An open, vendor-neutral network allows the state to choose from a variety of sources and select the most economical network solution without impacting applications.
- This approach supports economic and implementation flexibility because technology components can be purchased from many vendors. This insulates the state from unexpected changes in vendor strategies and capabilities.
- Applications should be designed to be transport-independent.

Principle 3.00.01.05 – User access should be a function of authentication and authorization, not of location.

Rationale:

- All users must obtain authentication via a user identification method consistent with the standards and usage guidelines set by the enterprise.
- Authorization of users must be performed according to the security rules of the enterprise and the local business unit.
- In order to perform their job functions, users need to access services available from multiple sites within the enterprise, from a variety of public and private networks, and from the Internet.

Technical Topic: Local Area Network

Best Practice 3.01.02.01 – Networks must be positioned for future growth in traffic and expansion of services such as voice and video.

Rationale:

- The increasing investment of funds in network infrastructures dictates that the life span of each additional component or enhancement be as long as possible. This can be accomplished if the design supports current needs but includes an anticipated growth potential. For example, installing Category 5 cabling today to run a 10mbps network positions a site to upgrade to a 100mbps speed in the future without replacing the cabling.
- As businesses expand, networks expand. A flexible, open network design will allow a business to minimize the costs and disruptions of configuration management while providing timely and responsive network changes when and where required.

Best Practice 3.01.02.02 – Configure all servers supporting mission critical applications, including desktop applications, to minimize service interruption.

Rationale:

- Select a computer constructed to perform as a highly available, highly reliable, fault tolerant server with such features as redundant disk arrays, network cards, power supplies, and processors.
- Select a server with sufficient growth capacity to accommodate the anticipated increase in application requirements over time. (See Platform Architecture.)
- Formalize security, disaster recovery, and backup procedures to ensure the integrity of both the server and the application. Test those practices on a regularly scheduled basis. (Refer to Systems Management and Security and Directory Services Architectures).

Standard 3.01.03.01 – The standard for LAN cabling is Category 5, 6, or 7 Unshielded Twisted Pair (Cat 5 UTP, Cat 6 UTP, or Cat 7 UTP).

Rationale:

- CAT 5/6/7 UTP can be certified to carry 10/100/1000 MBPS of data.
- It is a industry standard wiring plan and has the support of the IEEE.
- Wiring, cable, connector, and equipment vendors have standardized on this cabling.

Standard 3.01.03.02 – The standard for standard link layer access protocol is Ethernet, IEEE 802.3 Carrier Sense Multiple Access/Collision Detection Access Method (CSMA/CD).

Rationale:

- Widely accepted format.
- Reliable, the protocol has been used for years and is very stable.
- Scaleable, faster versions are currently emerging to help manage the increase of data flow.
- 1000BaseT Gigabit Ethernet has the bandwidth necessary to support the needs of future voice and video requirements.

Technical Topic: Wide Area Network

Best Practice 3.02.02.01 – Develop one enterprise-wide network infrastructure that is centrally maintained and managed.

Rationale:

- A single uniform network infrastructure allows an enterprise to respond more efficiently when faced with requests by agencies for WAN component upgrades and installation.
- A centrally developed and managed infrastructure provides a more cost effective use of infrastructure resources.
- Agencies or business units should focus their WAN requirements on functional specifications such as level of service needed, throughput needed, response time needed. The

implementation of an appropriately responsive WAN should be a specialized function performed for the enterprise in its entirety.

Best Practice 3.02.02.02 – When industry standards do not exist, use interim product standards.

Rationale:

- There currently are no industry standards established for all the components of WAN design. Therefore, a product-based standard provides for consistency in the development, deployment, and management of WAN technology.
- The cooperative, collaborative, and geometric nature of WANs mandates that standards be used in order to build a cohesive WAN environment. Size alone prohibits a totally random, variable structure.

Standard 3.02.03.01 – The standard protocol technology is TCP/IP.

Rationale:

- Open protocol.
- Allows Internet access.
- Allows creation of Intranets and VPNs.

Standard 3.02.03.02 – The standard internet access technology is Domain Name System (DNS) and IP address assignments are provided by State Information Technology Services (ITS) for those agencies participating in the North Carolina Integrated Information Network (NCIIN).

Rationale:

- ITS must assign IP addresses to allow LANs access to the NCIIN State WAN.
- All Internet access provided by the NCIIN and is controlled by the state's Domain Name System.
- It allows a structured naming conviction and IP address allocation for the state's WAN and domain names.

Technical Topic: Network-Centric Applications

Best Practice 3.03.02.01 – Include network expertise on the requirements and design teams.

Rationale:

- Including network expertise ensures correct planning, documentation, and standard practices are followed.
- Requirements definition should include application performance, as well as capacity planning for network usage (based on the predicted number and size of transactions).

- Define any special networking requirements or constraints and perform the associated network design before development tools are selected. Otherwise, the tools used may not support the network architecture required to support the business.
- The network can be modified (upgraded) while applications are under development.
- Performance and the cost to move information should be balanced during application design. Multiple perspectives of a cross-functional group can ensure all viable options are considered.

Best Practice 3.03.02.02 – Design network-neutral applications.

Rationale:

- Isolate the application code from the network specific code so business rules and data access code can be redeployed on a different platform, if necessary.
- Code to a middleware API, not to the network API.
- For a network to remain scaleable and portable, applications must be developed without regard to the type of network (i.e. WAN or LAN) they are to be deployed on.
- Network-specific design (e.g., wireless or guaranteed high-bandwidth) should only be performed when business requirements dictate.

Best Practice 3.03.02.03 – Minimize data movement.

Rationale:

- When possible, schedule heavy network use for off-peak hours. For example, where requirements for data freshness permit, perform database synchronization at night.
- Data warehouses typically are used for decision support applications requiring large amounts of data to be transferred through the network.
- When replicating databases, consider partitioning and distributing subsets, rather than duplicating the entire master database.
- Decoupling the application layers provides the most efficient use of network resources by allowing the data access layer to be placed near the data.

Best Practice 3.03.02.04 – Consider the impact of middleware on network utilization.

Rationale:

- Perform all transaction commits locally, between the resource manager and the queue. Asynchronous store and forward messaging can limit the scope of a transaction. (See Figure 3-7.)
- Decouple transactions as allowed by business rules. Reconcile data at low-cost times.
- Using store and forward, work can occur at a site even if the network link is down.

Best Practice 3.03.02.05 – When data has to be distributed to multiple points (e.g., software and content distribution), move it once and only once across each data link.

Rationale:

- Use push technology, rather than using client polling. It overloads servers and network links to servers.
- Use multicast, rather than broadcast, to distribute messages to multiple points.

Best Practice 3.03.02.06 – When designing distributed applications, make no assumptions about the speed of the network on which the application will be deployed.

Rationale:

Since bandwidth is unpredictable at design time:

- Minimize the amount of data to be moved between components. This will enhance performance regardless of the speed of the network on which the application is deployed.
- Use asynchronous rather than synchronous communications between application components (except in cases where business rules require synchronous communications). This will prevent application components waiting for a response from a server.
- For users and application requests that may be intermittently connected, use store-and-forward messaging to communicate with application components.
- When multiple, independent units of work must be performed, initiate all so they can be performed in parallel, rather than waiting for the completion of one before initiating the next.

Best Practice 3.03.02.07 – Perform performance measurement and load testing on distributed applications before deployment.

Rationale:

- Measure application performance often, especially before and after any component is moved to a different platform. This helps quantify the performance impact of the redeployment, and helps isolate any problems associated with a network link or platform.
- Use load testing tools that simulate many users accessing the application. This testing method will provide information that will not surface during single user test scenarios.
- Load testing will identify network bottlenecks (and application bottlenecks) before the application is deployed in the production environment.

Best Practice 3.03.02.08 – Deploy heavily used data sources "close" to the applications using them.

Rationale:

- "Close" does not imply physical proximity. It means deployed on platforms that have high-bandwidth connections between them. Do not perform heavy data movement across the WAN during peak hours.
- One of the biggest cost factors in designing a network is the transmission of the data over the communications system.
- For applications requiring very large amounts of data movement, try scheduling the execution of these queries to run during off peak hours to minimize the impact on network performance.

Technical Topic: Directory Services

Best Practice 3.05.02.01 – Implement a fault tolerant solution to provide 24-hour, 7-day availability to the enterprise directory.

Rationale:

- If the directory becomes inaccessible, the resources to which a user has rights become unavailable. Therefore, a directory mus be available at all times to accept authentication requests. This can be accomplished with a planned fail-over strategy to ensure that, if one server fails, another backup server can pick up the requests. This should include a replication strategy with hardware solutions that include disk or system duplexing, disk or system mirroring, disk arrays, and UPSs.

Best Practice 3.05.02.02 – Purchased applications and operating systems should be directory enabled.

Rationale:

- Securing applications and their operating environments is a significant challenge. Security is a naturalenvironment for the use of a directory. Applications can authenticate users to an external source by being directory enabled. The directory is better suited to provide information on the level of security necessary.
- Applications can be further enhanced when they are enabled to obtain an expanded set of information from the directory as appropriate. Thus making applications more modular and consolidating administration to a central location. For example, an application can gather employee information from the user object in the directory. This facilitates user authentication and authorization by making the resources on that platform available to the enterprise, when the appropriate rights are in place.

Standard 3.05.03.01 – Use the statewide directory services infrastructure.

Rationale:

Using the statewide directory services has several benefits:

- The infrastructure is simplified by providing a common interface to view and manage all available resources.
- Directory services are a critical component to statewide initiatives like E-mail and Electronic Commerce. The current enterprise directory is fault tolerant and highly available from any location that participates. Time,distance, and location do not restrict access to the information contained within the services.
- Coordinated directory services will improve communication between our applications, databases, and network operating systems by providing consistent, reliable information in an efficient and effective manner.

Standard 3.05.03.02 – Use the statewide directory services (NDS) for in-house developed applications to authenticate users.

Rationale:

- Novell NDS has become the State's de Facto standard for enterprise directory services. This has been a successful, well-coordinated effort that has been recognized internationally. NDS is available on severalplatforms such as Microsoft NT, Sun Solaris, and many others. NDS also supports numerous access protocols such as LDAP, ODBC, Java, and ActiveX. Implementing NDS on the available platforms, using the supported access protocols, will achieve interoperability between these platforms and applications. It will also provide a single point of administration and authentication. Participation in the Statewide NDS tree is required for those NDS installations within the NCIIN whether from NDS on NetWare or NDS on the other available platforms. Where NDS is not currently available, such as in the mainframe environment, use the Service Broker security services for authentication.
- In an enterprise environment, issues such as server naming conventions, net ids, tree structures, etc. must be carefully coordinated and adhered to. These have been addressed in documents under F. Resources -Distributed Computing Standards and Guidelines in this document.

Standard 3.05.03.03 – Integrate homogeneous directories into a single tree.

Rationale:

- It is more efficient to link "like" directories into a single tree. Most vendors of directories have implemented either the standards that currently exist or standards that have been proposed. These standards include a mechanism to connect their directories together to build a single tree. This provides the optimum integration of Public Agency resources and people without regard to location. A single tree minimizes infrastructure costs while maximizing the potential for agencies to choose how they share resources with other agencies including local governments. The single tree approach also allows for improved fault tolerance and better performance especially for agencies with geographically dispersed operations. Joining a tree, regardless of manufacturer, must be coordinated with Information Technology Services.
- It is necessary to tie these single trees from various manufacturers to the authoritative enterprise directory in order to provide authentication services to the authoritative enterprise directory. However, achievingconnectivity from one manufacturer's directory to another is complex and difficult. For example, tying one Netscape directory to Novell's NDS can be done but is difficult to implement and maintain. The state currently has dozens of Netscape directories in place. The process would then need to be performed for each of them. However, tying all Netscape directories together into a single tree is fairly straightforward and facilitated through their product. Then the one Netscape tree can be tied to the one NDS tree. It is a complicated task but it is performed once. Through the Enterprise Directory Services Initiative, this interoperability between dissimilar directories will be implemented. This will be accomplished through the use of meta-directory technologies.

Standard 3.05.03.04 – Use the North Carolina Service Broker (NCSB) services for directory functions.

Rationale:

- As in-house applications are developed, we must make use of the services that are already available rather than to constantly build new ones. An enterprise directory services infrastructure provides an addressable security service for authentication and authorization as well as a repository for digital certificates.
- These services are addressable directly from the enterprise directory or through a service via the North Carolina Service Broker. For more information about the North Carolina Service Broker, refer to the Componentware Architecture chapter.

Standard 3.05.03.05 – Use the Federated Metadata Repository directory schema attributes and object classes.

Rationale:

- A directory is basically a database that has been tuned to perform massive reads and infrequent writes. Like other databases in our enterprise, directories and their elements must be federated. For example, where a person object class may have an attribute of "Pager Number", "Pager Number" should be registered in the Federated Metadata Repository and populated according to that definition. Therefore, when the directory is queried for that information, the data returned will be as expected. In the past there has been a tendency to populate currently unused directory attributes with data that is not consistent with that attribute. For example, there may be a requirement to enter a pager number in the directory for a user. If there is no attribute for "Pager Number", there may be a tendency to select an attribute that is unused such as "Title". Instead, extend the schema to include a new attribute that precisely defines the data that will be placed there and register it with the Federated Metadata Repository. Do not store inconsistent information in an unused attribute.
- For more information about the Federated Metadata Repository, refer to the Data Domain.

Standard 3.05.03.06 – Use the State Novell NDS enterprise directory as the authoritative source for directory information.

Rationale:

- An enterprise directory is not a single directory product. It will be made up of several directories from several vendors. However, in an enterprise directory strategy one directory must be identified as the main directory and the authoritative source for all directory information. All other directories and applications in the enterprise look to it for complete re liable information.

Standard 3.05.03.07 – Populate directory objects according to the minimum attributes defined in Distributed Computing Standards and Guidelines.

Rationale:

- Any data source is only as good as the data it contains. If that data is missing, incorrect, or incomplete, the data source cannot be depended upon as an authoritative source for that type of information. A directory is no different. Directories have become much more than an authentication point for network users. In order to supply information on our users, network

devices, and organizations, directories must be built in as complete and reliable manner as possible.

- The object attributes for Novell NDS are listed and explained in the Distributed Computing Standards andGuidelines in the Novell Directory Services section at http://www.its.state.nc.us/About/Divisions/DCS/NDS/DistributedComputingStdsAndGuidelines.pdf The attributes are identified as Mandatory, Recommended, Optional, Unused, Automatic, Multi Valued, and Template.

Standard 3.05.03.08 – Use Lightweight Directory Access Protocol version 3 (LDAPv3) for directory access where strong security is not required.

Rationale:

- LDAPv3 is the industry standard lightweight access protocol and does not offer strong authentication or access controls. However, LDAPv3 can provide standards based access to directories for lookups, as a communication mechanism for synchronization tools, public key retrieval, and others. Commercial off-the-shelf (COTS) applications often require their own directories. Access to the application directory from outside or for the application to communicate with an external directory will require a standards based approach. Therefore, when purchasing CO TS applications, LDAPv3 compatibility is required. LDAPv3 also provides a standards based access to the directory for lookups, as a communication mechanism for synchronization tools, public key retrieval, and others.